NetAgent
ネットエージェント株式会社

プログラム解析による暗号通信文の解析方法

ネットエージェント株式会社
杉浦 隆幸

概要

NetAgent
ネットエージェント株式会社

- 日ごろ使っているソフトウェアがどのような通信をしているか知っていますか。実際は送りたくない情報を送っているかもしれません、送りたくないような情報を送っているようなソフトウェアほど、通信を暗号化し、技術的に何を送っているのかを解明することが難しくなっています。難しい部分もありますが、これらを判明させていく手法を順を追って紹介します。

- 独自プロトコルソフトは何を送っているのでしょうか？
  - メッセンジャー
  - ウイルス対策ソフトのデータ
  - ブラウザ以外のSSL通信
  - Winny、Share、SpkypeなどのP2Pソフトウェア
- クイズがあるので分かったら答えてください。

手法

NetAgent
ネットエージェント株式会社

- 手法１：パケットをキャプチャする
- 手法２：プロキシサーバ、中継サーバで記録する
- 手法３：プログラムのメモリイメージを見てみる
- 手法４：プログラムにディバッガを当てて暗号通信の使用部分に来たときのデータを見てみる。

対象

NetAgent
ネットエージェント株式会社

暗号通信をして情報を隠したいようなソフトってどんなのことをするソフト？

- スパイウェア
  - 変な動作をするソフトウェア
- ボット
  - 暗号化してボットネットにつながっている場合
- P2Pソフト
  - WinnyとかShareとかPerfect Darkとか

できる限り楽をして・・・

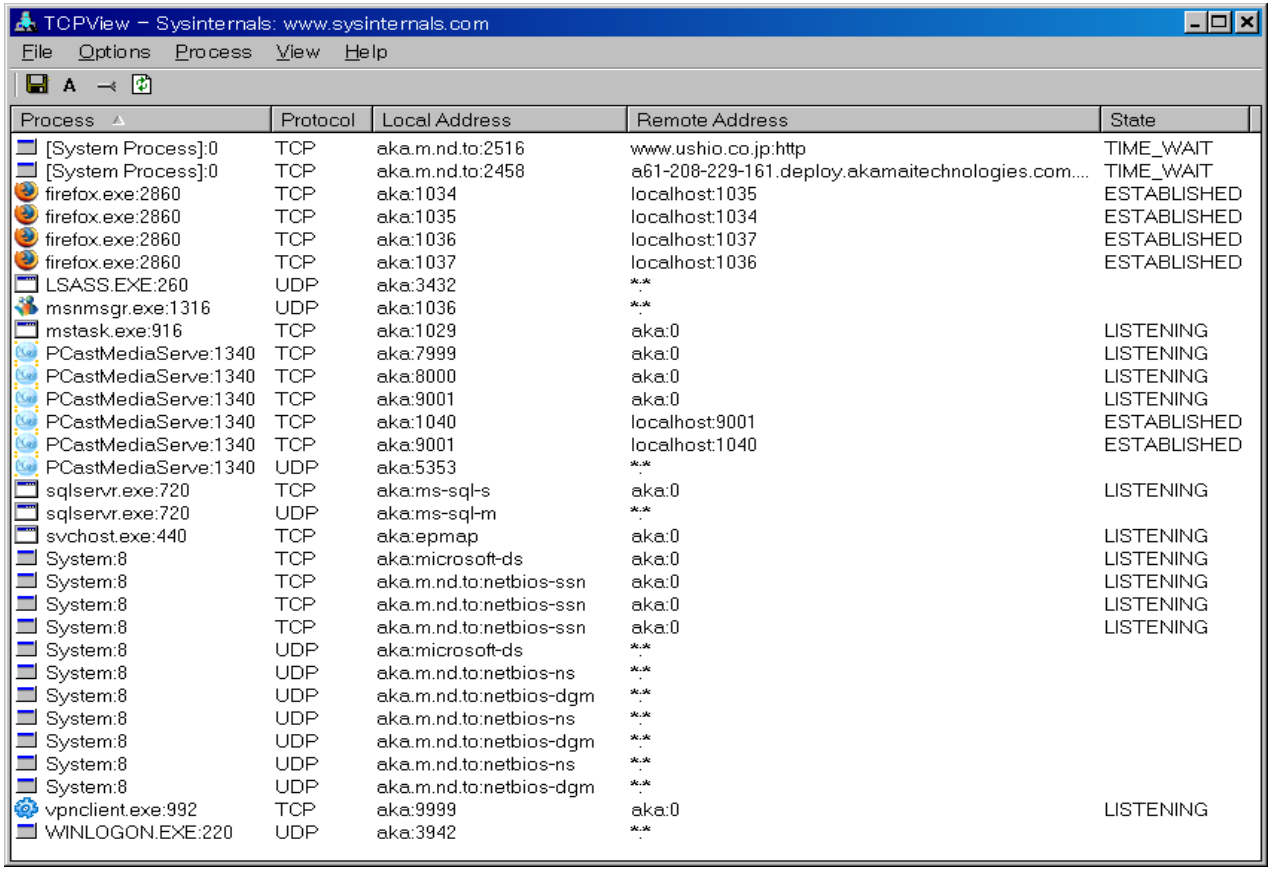
NetAgent
ネットエージェント株式会社

- 解析には段階がある。
  できれば楽な方法でやりたい。
  - 1. 平分通信ならパケットキャプチャで
  - 2. 実行ファイルの文字列にあるならstringsで
  - 3. プログラムのメモリイメージでよいならそれで
  - 4. ソースがあるのならそれを読んで
  - 5. 仕方ないので、バイナリのプログラムを解析して

パケットキャプチャの前に

NetAgent ネットエージェント株式会社

- TCPviewで調べるポート確認
- http://www.microsoft.com/technet/sysinternals/utilities/TcpView.mspx
    - 使っているプログラムがグラフィカルに出るnetstat

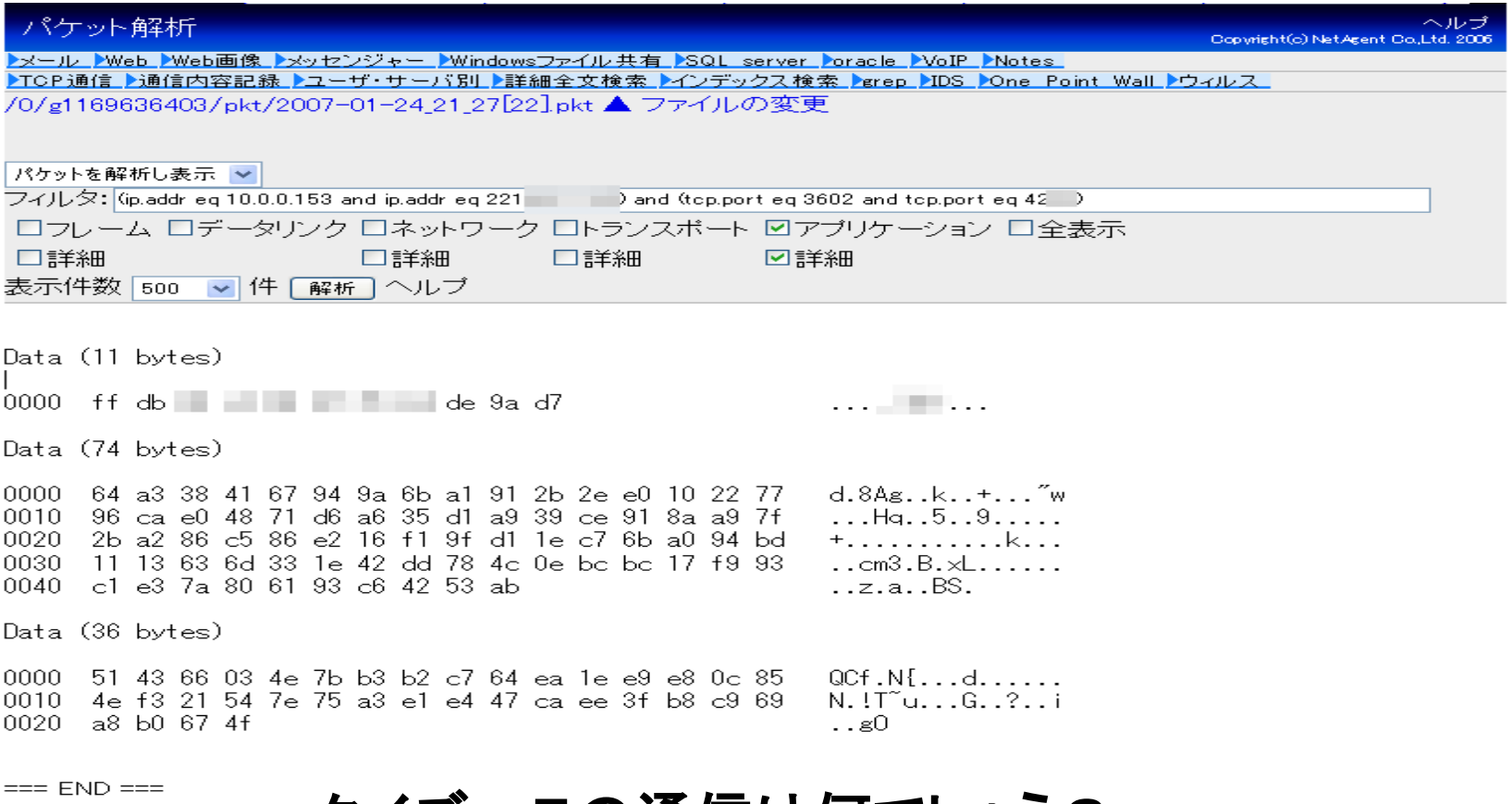

TCPView – Sysinternals: www.sysinternals.com

File Options Process View Help

Process	Protocol	Local Address	Remote Address	State
[System Process]:0	TCP	aka.m.nd.to:2516	www.ushio.co.jp:http	TIME_WAIT
[System Process]:0	TCP	aka.m.nd.to:2458	a61-208-229-161.deploy.akamaitechnologies.com....	TIME_WAIT
firefox.exe:2860	TCP	aka:1034	localhost:1035	ESTABLISHED
firefox.exe:2860	TCP	aka:1035	localhost:1034	ESTABLISHED
firefox.exe:2860	TCP	aka:1036	localhost:1037	ESTABLISHED
firefox.exe:2860	TCP	aka:1037	localhost:1036	ESTABLISHED
LSASS.EXE:260	UDP	aka:3432	*:*	
msnmsgr.exe:1316	UDP	aka:1036	*:*	
mstask.exe:916	TCP	aka:1029	aka:0	LISTENING
PCastMediaServe:1340	TCP	aka:7999	aka:0	LISTENING
PCastMediaServe:1340	TCP	aka:8000	aka:0	LISTENING
PCastMediaServe:1340	TCP	aka:9001	aka:0	LISTENING
PCastMediaServe:1340	TCP	aka:1040	localhost:9001	ESTABLISHED
PCastMediaServe:1340	TCP	aka:9001	localhost:1040	ESTABLISHED
PCastMediaServe:1340	UDP	aka:5353	*:*	
sqlservr.exe:720	TCP	aka:ms-sql-s	aka:0	LISTENING
sqlservr.exe:720	UDP	aka:ms-sql-m	*:*	
svchost.exe:440	TCP	aka:epmap	aka:0	LISTENING
System:8	TCP	aka:microsoft-ds	aka:0	LISTENING
System:8	TCP	aka.m.nd.to:netbios-ssn	aka:0	LISTENING
System:8	TCP	aka.m.nd.to:netbios-ssn	aka:0	LISTENING
System:8	TCP	aka.m.nd.to:netbios-ssn	aka:0	LISTENING
System:8	UDP	aka:microsoft-ds	*:*	
System:8	UDP	aka.m.nd.to:netbios-ns	*:*	
System:8	UDP	aka.m.nd.to:netbios-dgm	*:*	
System:8	UDP	aka.m.nd.to:netbios-ns	*:*	
System:8	UDP	aka.m.nd.to:netbios-dgm	*:*	
System:8	UDP	aka.m.nd.to:netbios-ns	*:*	
System:8	UDP	aka.m.nd.to:netbios-dgm	*:*	
vpnclient.exe:992	TCP	aka:9999	aka:0	LISTENING
WINLOGON.EXE:220	UDP	aka:3942	*:*	

パケットキャプチャ

ネットエージェント株式会社



クイズ：この通信は何でしょう？

パケットキャプチャ

NetAgent
ネットエージェント株式会社

•http://www.google-analytics.com/__utm.gif?utmwv=1&utmn=1208086912&utmcs=iso-2022-jp&utmsr=1280x1024&utmsc=32-bit&utmul=ja&utmje=1&utmfl=8.0&utmcn=1&utmdt=Sun%20Microsystems%20-%20%E3%82%A2%E3%83%97%E3%83%AA%E3%82%B1%E3%83%BC%E3%82%B7%E3%83%A7%E3%83%B3%E3%81%AE%E6%8B%A1%E5%BC%B5&utmhn=jp.sun.com&utmr=http://www.google.co.jp/search?hl=ja&q=off_t&btnG=Google+%E6%A4%9C%E7%B4%A2&lr=lang_ja&utmp=/products/software/solaris/wp/Sol_file/sol_3.html&utmac=UA-150017-1&utmcc=__utma%3D164123876.1208086912.1169641053.1169641053.1169641053.1%3B%2B__utmb%3D164123876%3B%2B__utmc%3D164123876%3B%2B__utmz%3D164123876.1169641053.1.1.utmccn%3D(organic)%7Cutmcsr%3Dgoogle%7Cutmctr%3Doff_t%7Cutmcmd%3Dorganic%3B%2B

妙に長いアクセス

結果 ⟶

パケットキャプチャ

ネットエージェント株式会社

Googleのトラッキング用のURL
で透過1x1ピクセルの画像表示

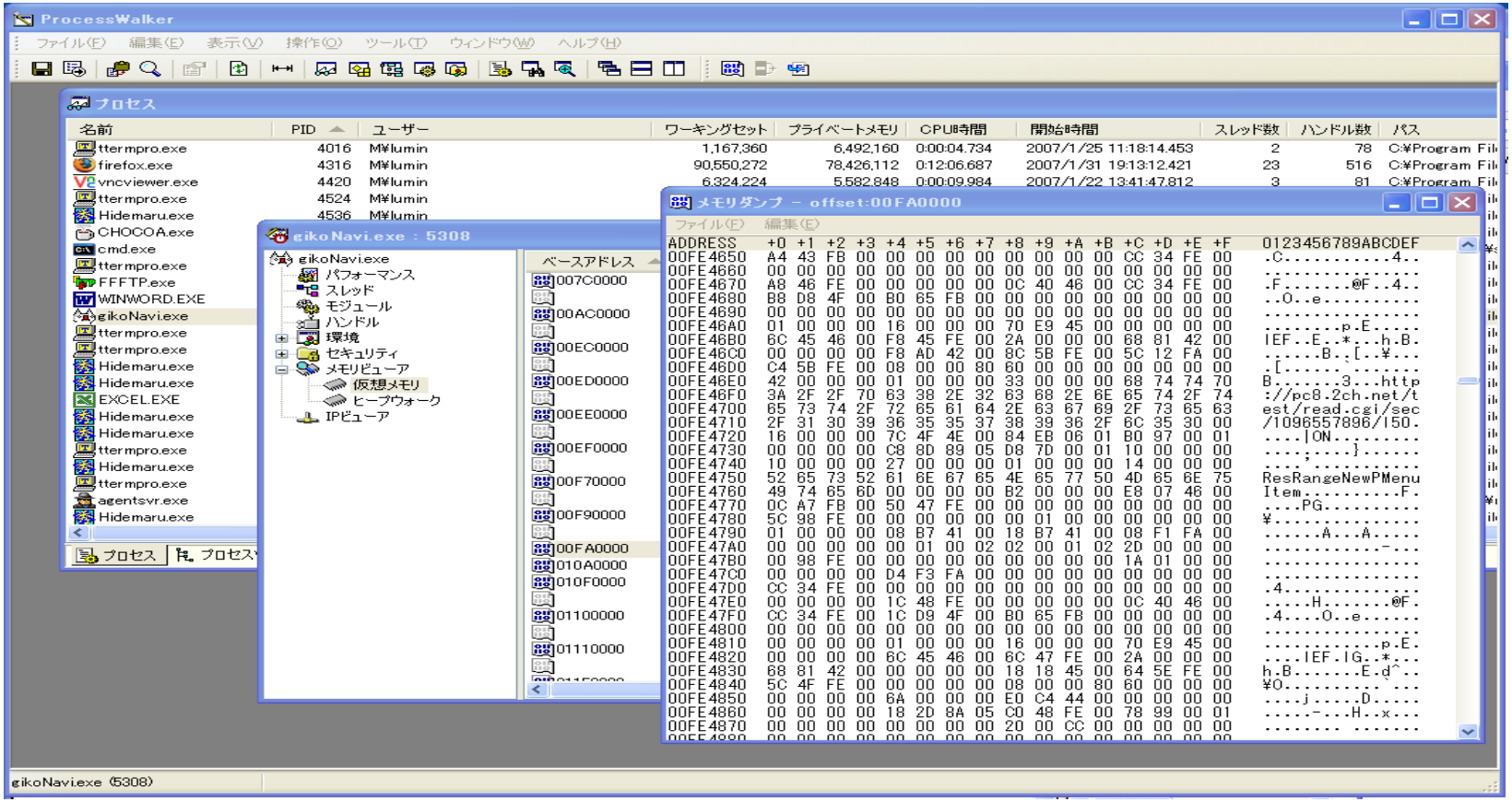
```
POST
utmwv=1
utmn=1208086912
utmcs=iso-2022-jp
utmsr=1280x1024
utmsc=32-bit
utmul=ja
utmje=1
utmfl=8.0
utmcn=1
utmdt=Sun Microsystems - アプリケーションの拡張
utmhn=jp.sun.com
utmr=http://www.google.co.jp/search?hl=ja
q=off_t
btnG=Google 検索
lr=lang_ja
utmp=/products/software/solaris/wp/Sol_file/sol_3.html
utmac=UA-150017-1
utmcc=__utma=164123876.1208086912.1169641053.1169641053.116964105
```

プログラムのメモリイメージを解析

- 実際にやってみましょう。
- ProcessWalkerか、Ollydbgを使います

今日来た人が見られる特典です。

プログラムのメモリイメージを解析



プログラム解析ツール

NetAgent
ネットエージェント株式会社

- ollydbg (free)
  - http://www.ollydbg.de/
- IDA Pro　(470 USD or 895 USD)
  - http://www.datarescue.com/
  - FAXを送ってクレジットカードで買う
- プログラム言語 (cとかperlとか)

プログラム解析を始めよう！

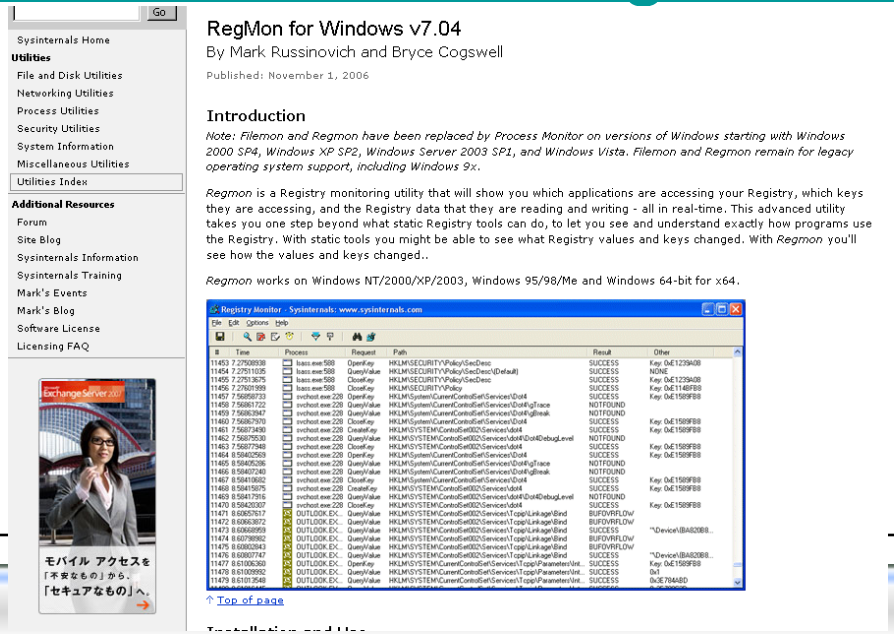
NetAgent
ネットエージェント株式会社

- まずは楽にできるところから
  - Regmon, filemon

レジストリの読み書きを確認

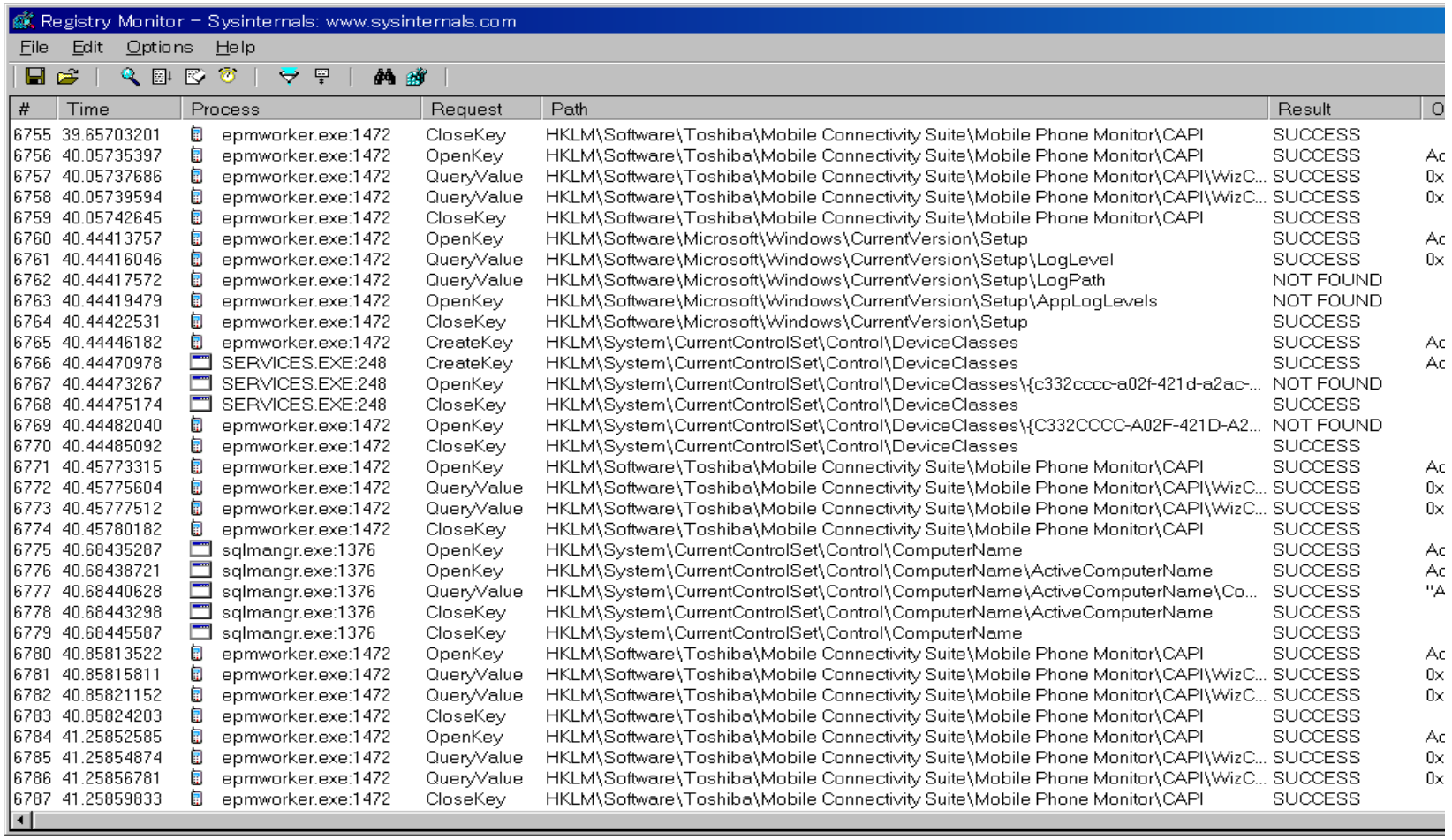
Net Agent
ネットエージェント株式会社

- Regmon
- http://www.microsoft.com/technet/sysinternals/utilities/Regmon.mspx



regmon

NetAgent
ネットエージェント株式会社


Registry Monitor – Sysinternals: www.sysinternals.com

File Edit Options Help

#	Time	Process	Request	Path	Result	O
6755	39.65703201	epmworker.exe:1472	CloseKey	HKLM\Software\Toshiba\Mobile Connectivity Suite\Mobile Phone Monitor\CAPI	SUCCESS	
6756	40.05735397	epmworker.exe:1472	OpenKey	HKLM\Software\Toshiba\Mobile Connectivity Suite\Mobile Phone Monitor\CAPI	SUCCESS	Ac
6757	40.05737686	epmworker.exe:1472	QueryValue	HKLM\Software\Toshiba\Mobile Connectivity Suite\Mobile Phone Monitor\CAPI\WizC...	SUCCESS	0x
6758	40.05739594	epmworker.exe:1472	QueryValue	HKLM\Software\Toshiba\Mobile Connectivity Suite\Mobile Phone Monitor\CAPI\WizC...	SUCCESS	0x
6759	40.05742645	epmworker.exe:1472	CloseKey	HKLM\Software\Toshiba\Mobile Connectivity Suite\Mobile Phone Monitor\CAPI	SUCCESS	
6760	40.44413757	epmworker.exe:1472	OpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	SUCCESS	Ac
6761	40.44416046	epmworker.exe:1472	QueryValue	HKLM\Software\Microsoft\Windows\CurrentVersion\Setup\LogLevel	SUCCESS	0x
6762	40.44417572	epmworker.exe:1472	QueryValue	HKLM\Software\Microsoft\Windows\CurrentVersion\Setup\LogPath	NOT FOUND	
6763	40.44419479	epmworker.exe:1472	OpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\Setup\AppLogLevels	NOT FOUND	
6764	40.44422531	epmworker.exe:1472	CloseKey	HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	SUCCESS	
6765	40.44446182	epmworker.exe:1472	CreateKey	HKLM\System\CurrentControlSet\Control\DeviceClasses	SUCCESS	Ac
6766	40.44470978	SERVICES.EXE:248	CreateKey	HKLM\System\CurrentControlSet\Control\DeviceClasses	SUCCESS	Ac
6767	40.44473267	SERVICES.EXE:248	OpenKey	HKLM\System\CurrentControlSet\Control\DeviceClasses\{c332cccc-a02f-421d-a2ac-...	NOT FOUND	
6768	40.44475174	SERVICES.EXE:248	CloseKey	HKLM\System\CurrentControlSet\Control\DeviceClasses	SUCCESS	
6769	40.44482040	epmworker.exe:1472	OpenKey	HKLM\System\CurrentControlSet\Control\DeviceClasses\{C332CCCC-A02F-421D-A2...	NOT FOUND	
6770	40.44485092	epmworker.exe:1472	CloseKey	HKLM\System\CurrentControlSet\Control\DeviceClasses	SUCCESS	
6771	40.45773315	epmworker.exe:1472	OpenKey	HKLM\Software\Toshiba\Mobile Connectivity Suite\Mobile Phone Monitor\CAPI	SUCCESS	Ac
6772	40.45775604	epmworker.exe:1472	QueryValue	HKLM\Software\Toshiba\Mobile Connectivity Suite\Mobile Phone Monitor\CAPI\WizC...	SUCCESS	0x
6773	40.45777512	epmworker.exe:1472	QueryValue	HKLM\Software\Toshiba\Mobile Connectivity Suite\Mobile Phone Monitor\CAPI\WizC...	SUCCESS	0x
6774	40.45780182	epmworker.exe:1472	CloseKey	HKLM\Software\Toshiba\Mobile Connectivity Suite\Mobile Phone Monitor\CAPI	SUCCESS	
6775	40.68435287	sqlmangr.exe:1376	OpenKey	HKLM\System\CurrentControlSet\Control\ComputerName	SUCCESS	Ac
6776	40.68438721	sqlmangr.exe:1376	OpenKey	HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	SUCCESS	Ac
6777	40.68440628	sqlmangr.exe:1376	QueryValue	HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\Co...	SUCCESS	"A
6778	40.68443298	sqlmangr.exe:1376	CloseKey	HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	SUCCESS	
6779	40.68445587	sqlmangr.exe:1376	CloseKey	HKLM\System\CurrentControlSet\Control\ComputerName	SUCCESS	
6780	40.85813522	epmworker.exe:1472	OpenKey	HKLM\Software\Toshiba\Mobile Connectivity Suite\Mobile Phone Monitor\CAPI	SUCCESS	Ac
6781	40.85815811	epmworker.exe:1472	QueryValue	HKLM\Software\Toshiba\Mobile Connectivity Suite\Mobile Phone Monitor\CAPI\WizC...	SUCCESS	0x
6782	40.85821152	epmworker.exe:1472	QueryValue	HKLM\Software\Toshiba\Mobile Connectivity Suite\Mobile Phone Monitor\CAPI\WizC...	SUCCESS	0x
6783	40.85824203	epmworker.exe:1472	CloseKey	HKLM\Software\Toshiba\Mobile Connectivity Suite\Mobile Phone Monitor\CAPI	SUCCESS	
6784	41.25852585	epmworker.exe:1472	OpenKey	HKLM\Software\Toshiba\Mobile Connectivity Suite\Mobile Phone Monitor\CAPI	SUCCESS	Ac
6785	41.25854874	epmworker.exe:1472	QueryValue	HKLM\Software\Toshiba\Mobile Connectivity Suite\Mobile Phone Monitor\CAPI\WizC...	SUCCESS	0x
6786	41.25856781	epmworker.exe:1472	QueryValue	HKLM\Software\Toshiba\Mobile Connectivity Suite\Mobile Phone Monitor\CAPI\WizC...	SUCCESS	0x
6787	41.25859833	epmworker.exe:1472	CloseKey	HKLM\Software\Toshiba\Mobile Connectivity Suite\Mobile Phone Monitor\CAPI	SUCCESS	

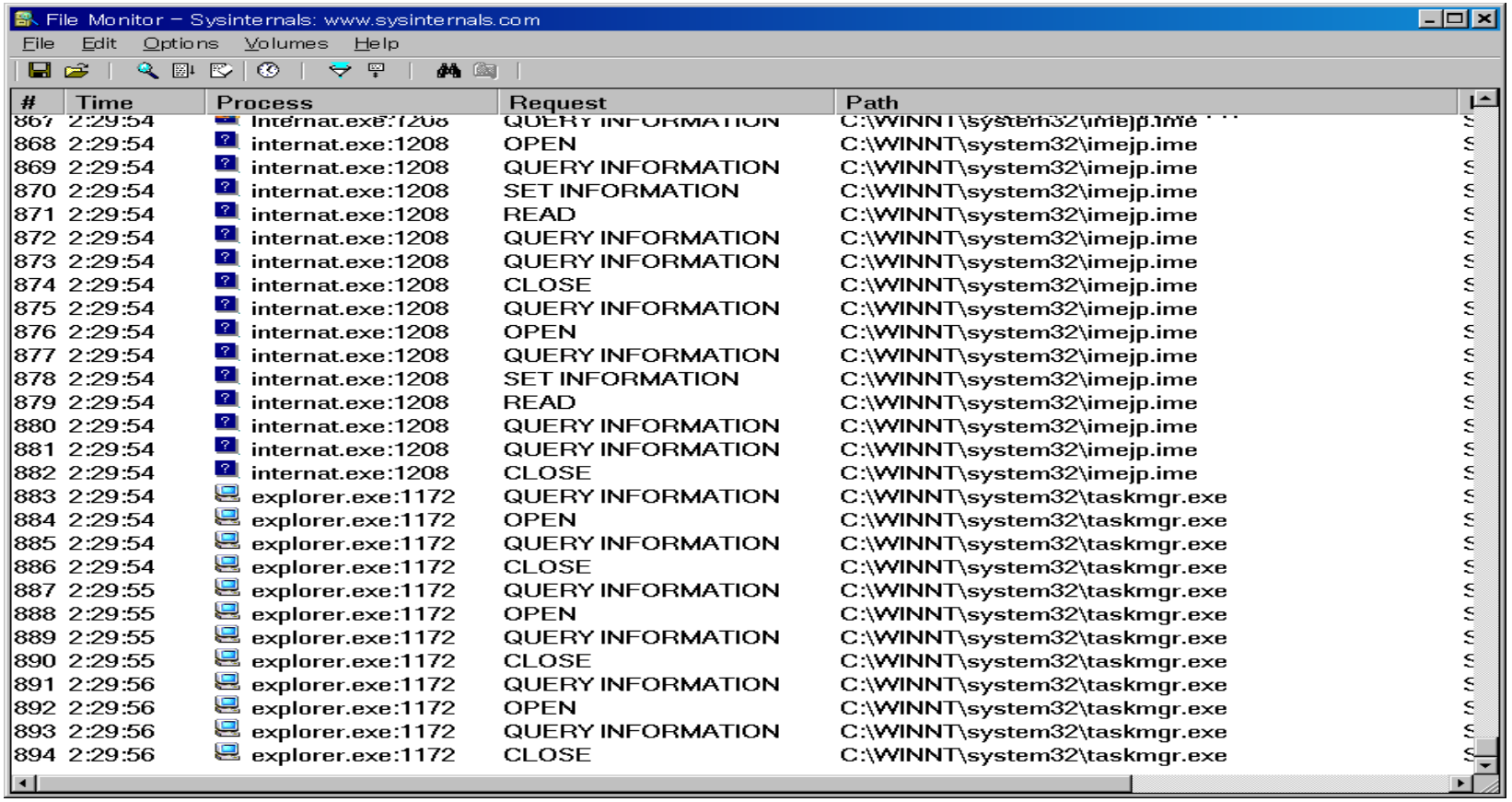
ファイルの読み書きを確認

NetAgent ネットエージェント株式会社

- Filemon
- http://www.microsoft.com/technet/sysinternals/SystemInformation/Filemon.mspx

filemon

NetAgent
ネットエージェント株式会社



プロセスの状態を取得

NetAgent
ネットエージェント株式会社

- Process walker
  - DLLやメモリイメージが見られるので、
  - 通信内容が平文で存在したらすぐにわかる。

うさみみハリケーン

NetAgent
ネットエージェント株式会社

- PEヘッダの解析
- リソース解析
- DLLからのインポート関数一覧表示

スタティック解析（IDA Pro）

NetAgent
ネットエージェント株式会社

- 実行ファイル、DLL、ocx等を読み込むと、1000～10000ぐらいのサブルーチンに分けてくれるので、それを1つ1つ読んでいく。

- IDA Proを使ってみよう

実際にデモしてみます

書かれた言語を知る

NetAgent
ネットエージェント株式会社

Functions window

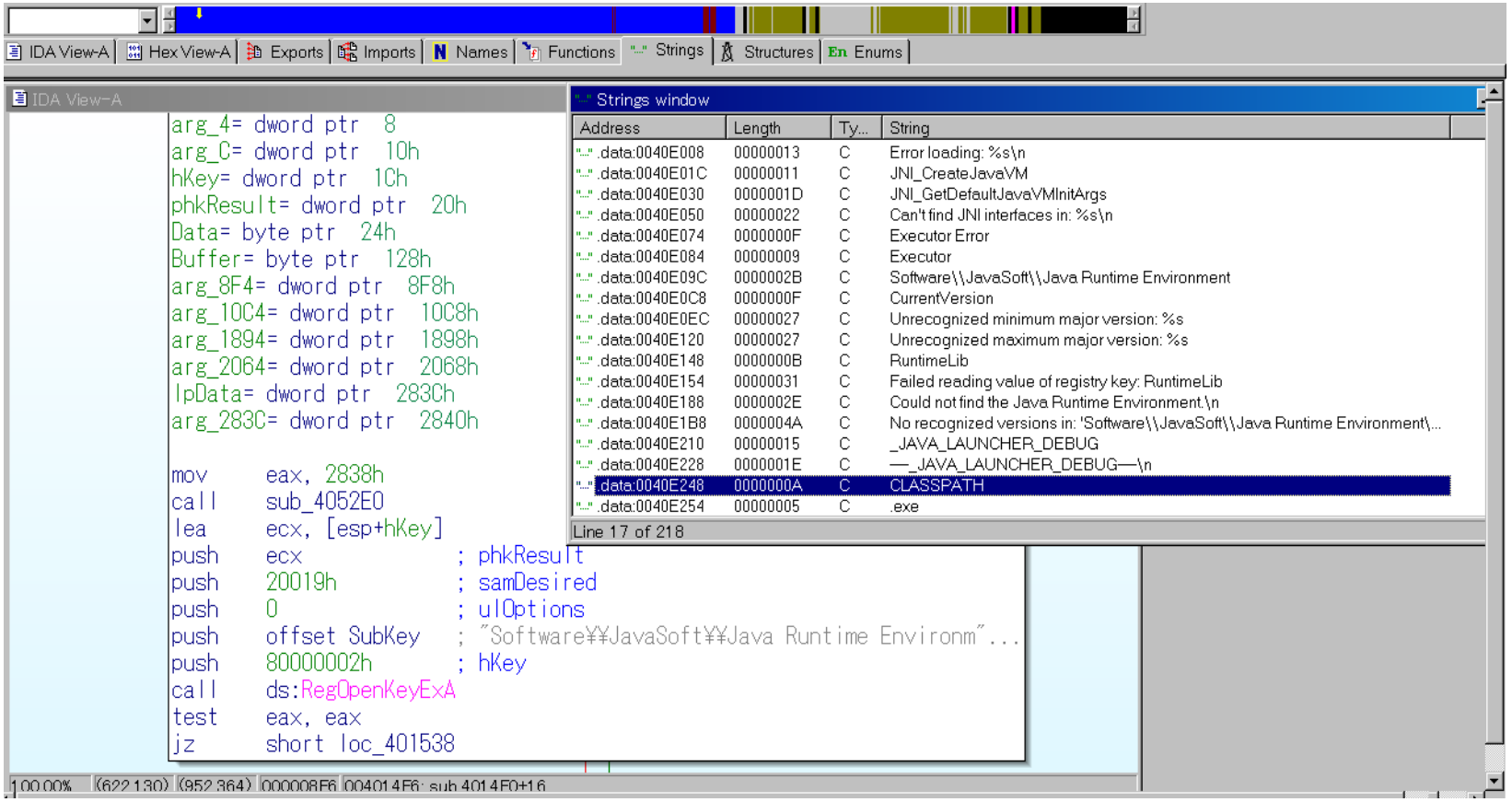
Function name	Segment	Start	Length	R	F	L	S	B	T
FolderItemCreateAsFolder	.text	00427D40	00000045	R	.	.	.	B	.
FolderItemGroupGetter	.text	00427D90	0000006A	R	.	.	.	B	.
FolderItemGroupSetter	.text	00427E00	00000079	R	.	.	.	B	.
FolderItemOwnerGetter	.text	00427E80	0000006A	R	.	.	.	B	.
FolderItemOwnerSetter	.text	00427EF0	00000079	R	.	.	.	B	.
FolderItemLaunch	.text	00427F70	00000047	R	.	.	.	B	.
FolderItemMoveFileTo	.text	00427FC0	00000085	R	.	.	.	B	.
FolderItemCopyFileTo	.text	00428050	00000085	R	.	.	.	B	.
FolderItemOpenImage	.text	004280E0	00000049	R	.	.	.	B	.
FolderItemOpenVectorImage	.text	00428130	00000049	R	.	.	.	B	.
FolderItemOpenSound	.text	00428180	00000074	R	.	.	.	B	.
FolderItemOpenMovie	.text	00428200	00000047	R	.	.	.	B	.
FolderItemOpenResourceMovie	.text	00428250	00000056	R	.	.	.	B	.
FolderItemOpenStyledEditField	.text	004282B0	00000048	R	.	.	.	B	.
FolderItemSaveStyledEditField	.text	00428300	00000048	R	.	.	.	B	.
FolderItemOpenBinaryFile	.text	00428350	0000008A	R	.	.	.	B	.
FolderItemCreateBinaryFile	.text	004283E0	000000C6	R	.	.	.	B	.
FolderItemSaveAsPicture	.text	004284B0	0000004B	R	.	.	.	B	.
folderParentGetter	.text	00428500	00000082	R	.	.	.	B	.
folderFindFolder	.text	00428590	0000007E	R	.	.	.	B	.
fileAbsolutePathGetter	.text	00428610	00000063	R	.	.	.	B	.
sub_428680	.text	00428680	000002AC	R	.	.	.	B	.
sub_428930	.text	00428930	00000047	R	.	.	.	B	.
sub_428980	.text	00428980	000000C1	R	.	.	.	B	.
sub_428A50	.text	00428A50	0000031A	R	.	.	.	B	.
RuntimeGetFolderItem	.text	00428D70	00000017	R	.	.	.	B	.
RuntimeGetTrueFolderItem	.text	00428D90	00000017	R	.	.	.	B	.

Line 1059 of 6668

クイズ： このプログラムの書かれた言語を当ててみましょう。

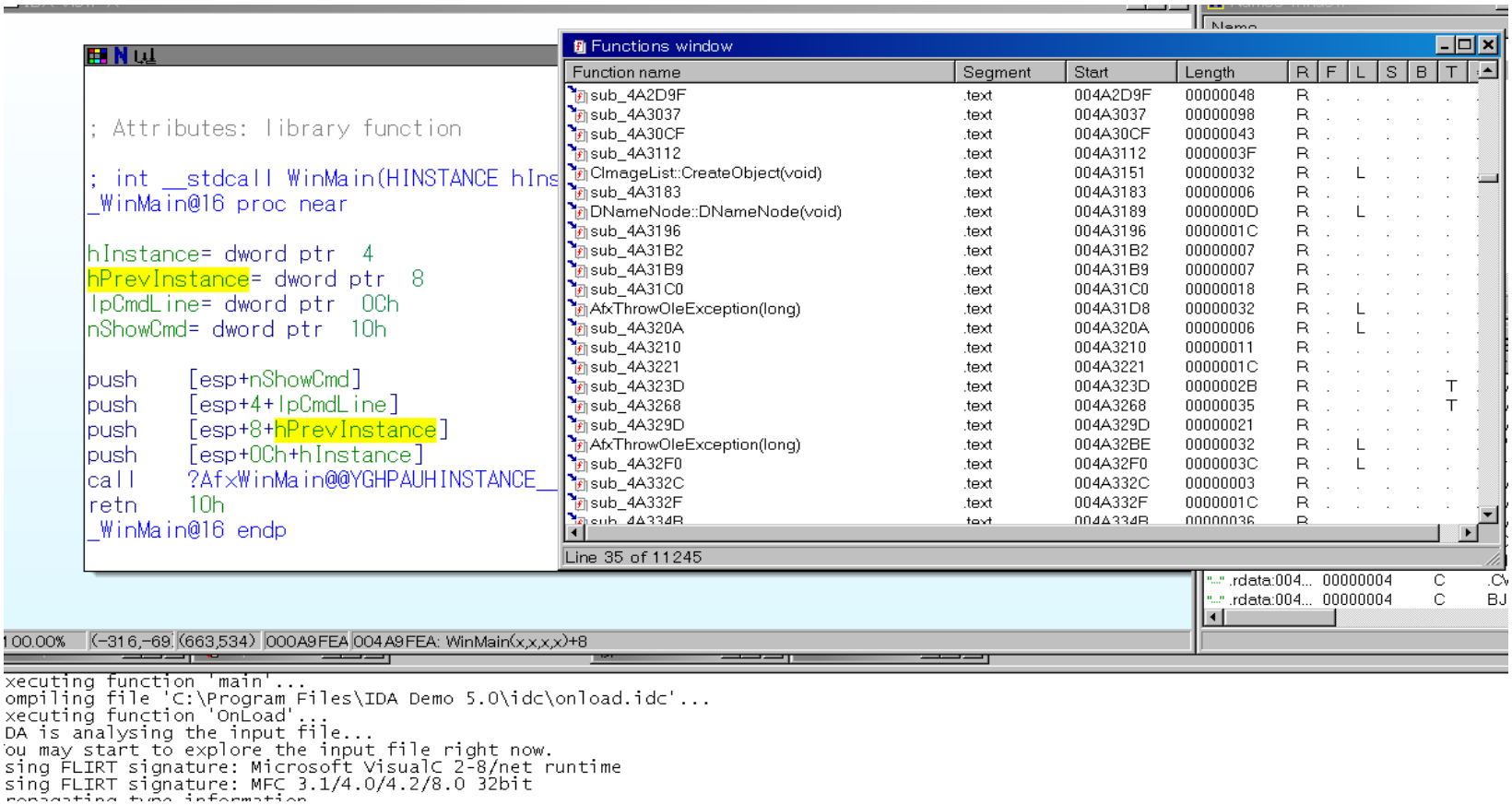
Javaバイナリ

ネットエージェント株式会社

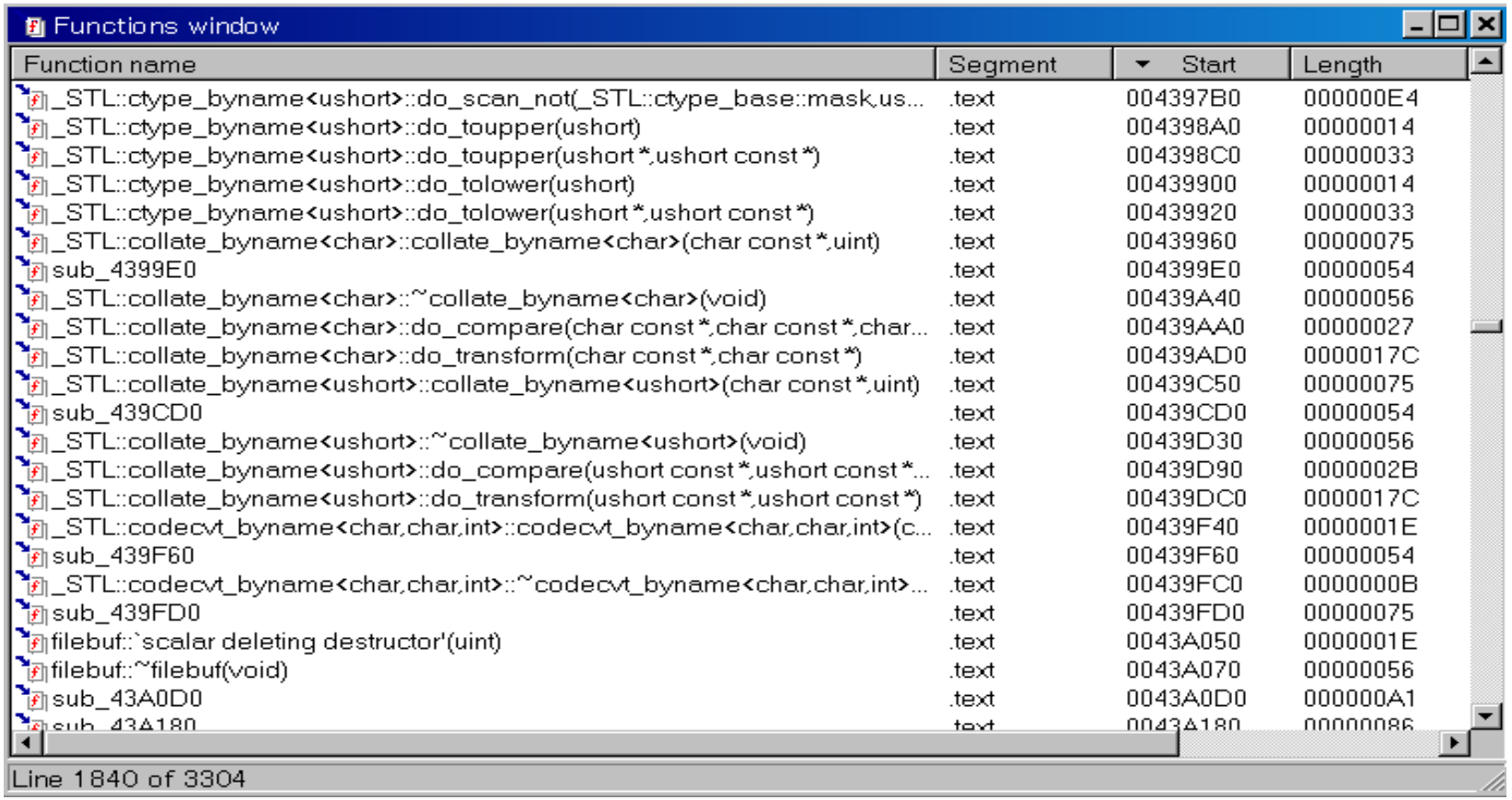


VC++

NetAgent
ネットエージェント株式会社

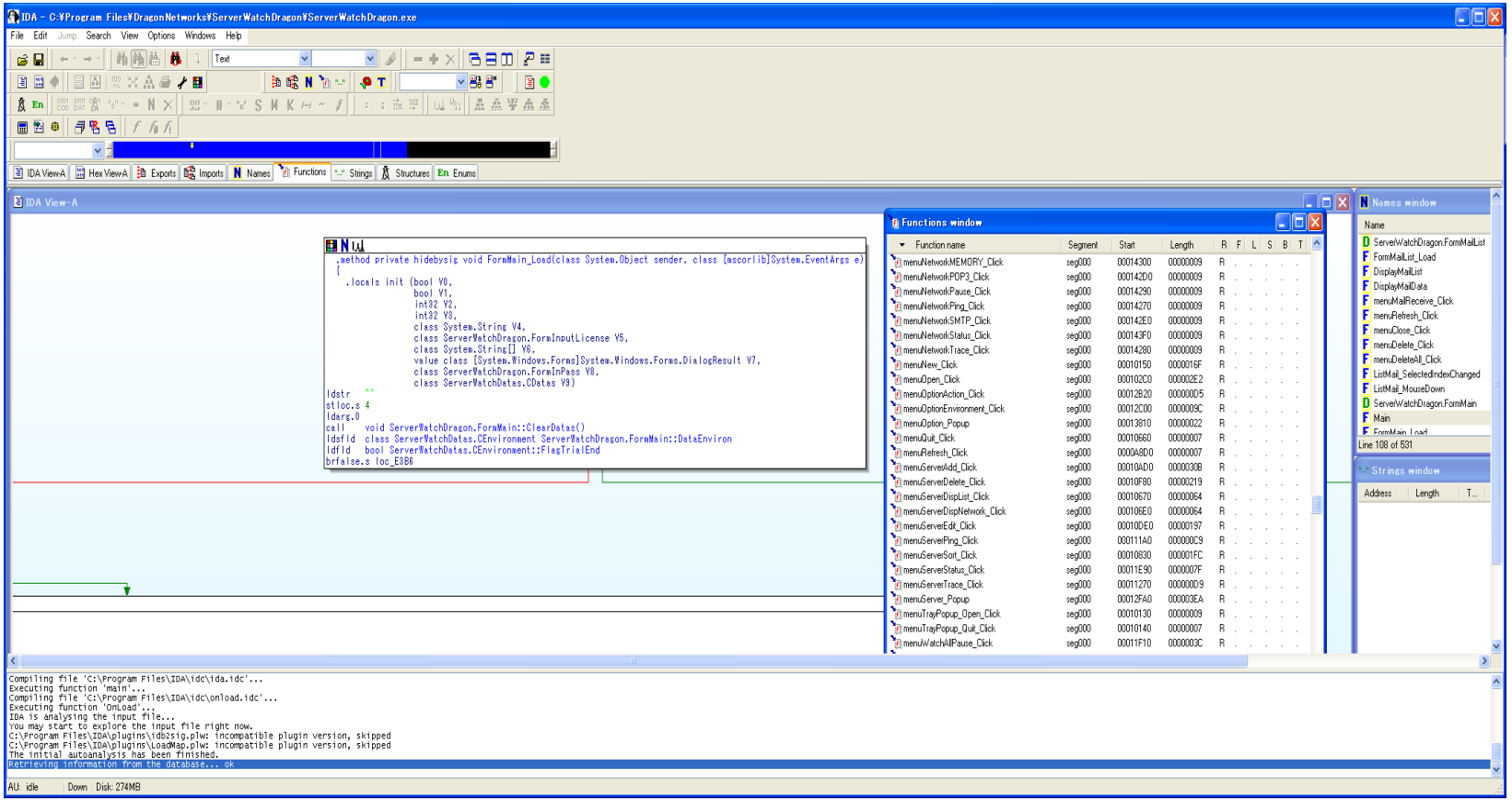


NetAgent
ネットエージェント株式会社



C#/VB .NET

NetAgent
ネットエージェント株式会社



判断方法

NetAgent
ネットエージェント株式会社

- 各言語の特徴が出る
- Stringで入っているのでそこを見る
- バイナリエディッタでプログラムの最後のXMLを見る
- PEid(後述)を使う
  - 一番楽に結果が出ます

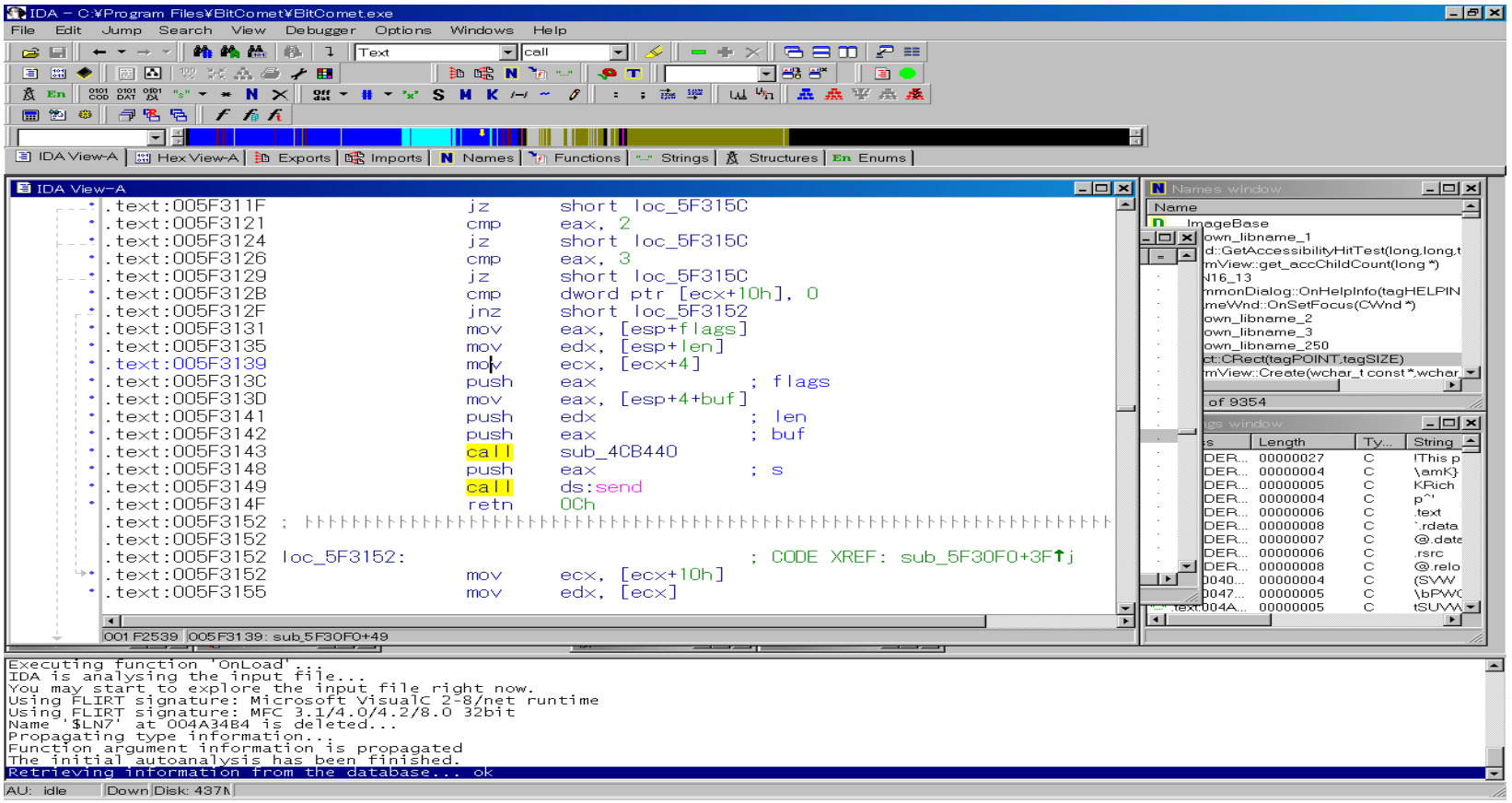
通信箇所を探す

NetAgent
ネットエージェント株式会社

- 目的は通信なので send() recv() を探してそこからたどるのみ。

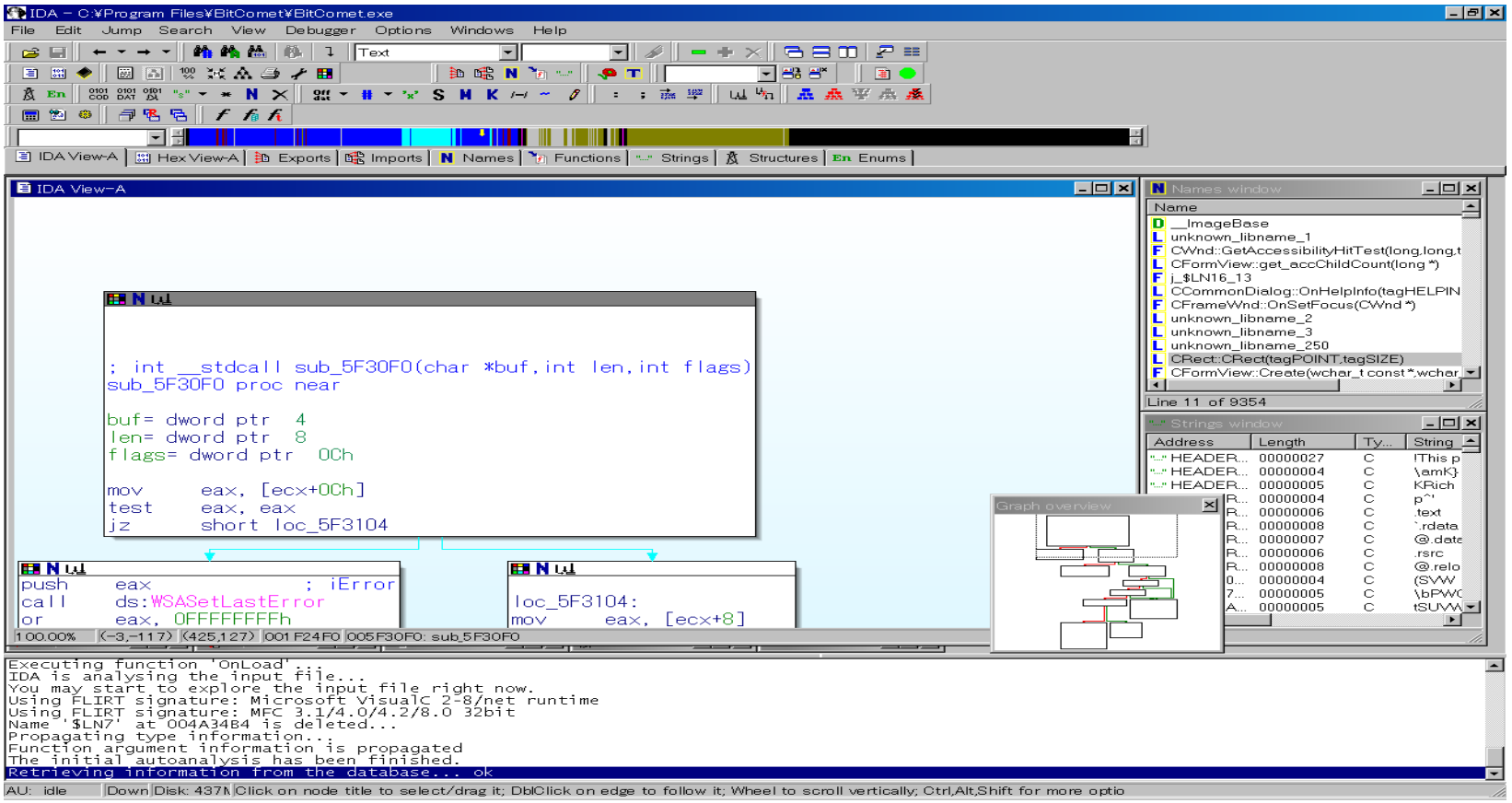
Send 発見

ネットエージェント株式会社



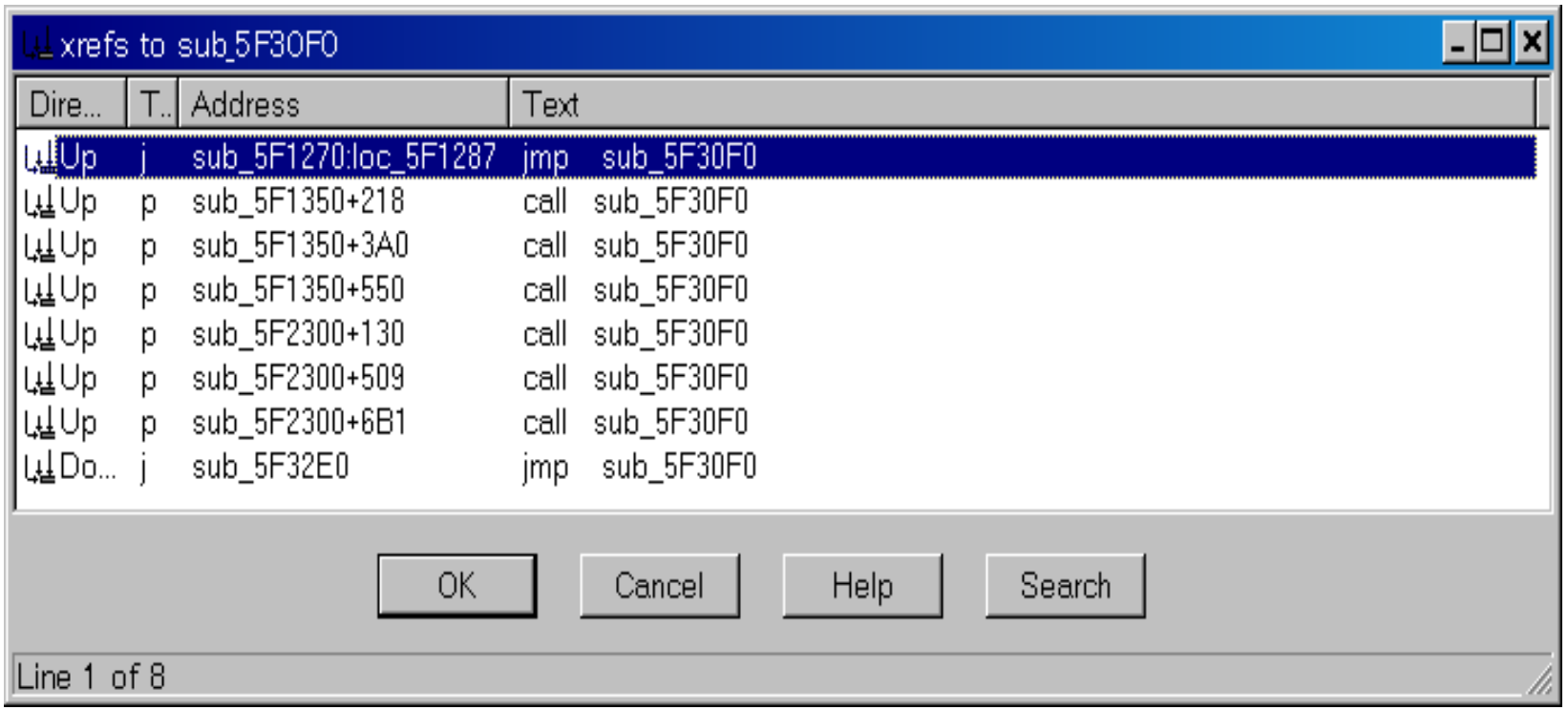
Sendを呼んでいるところのパラメータ

NetAgent
ネットエージェント株式会社



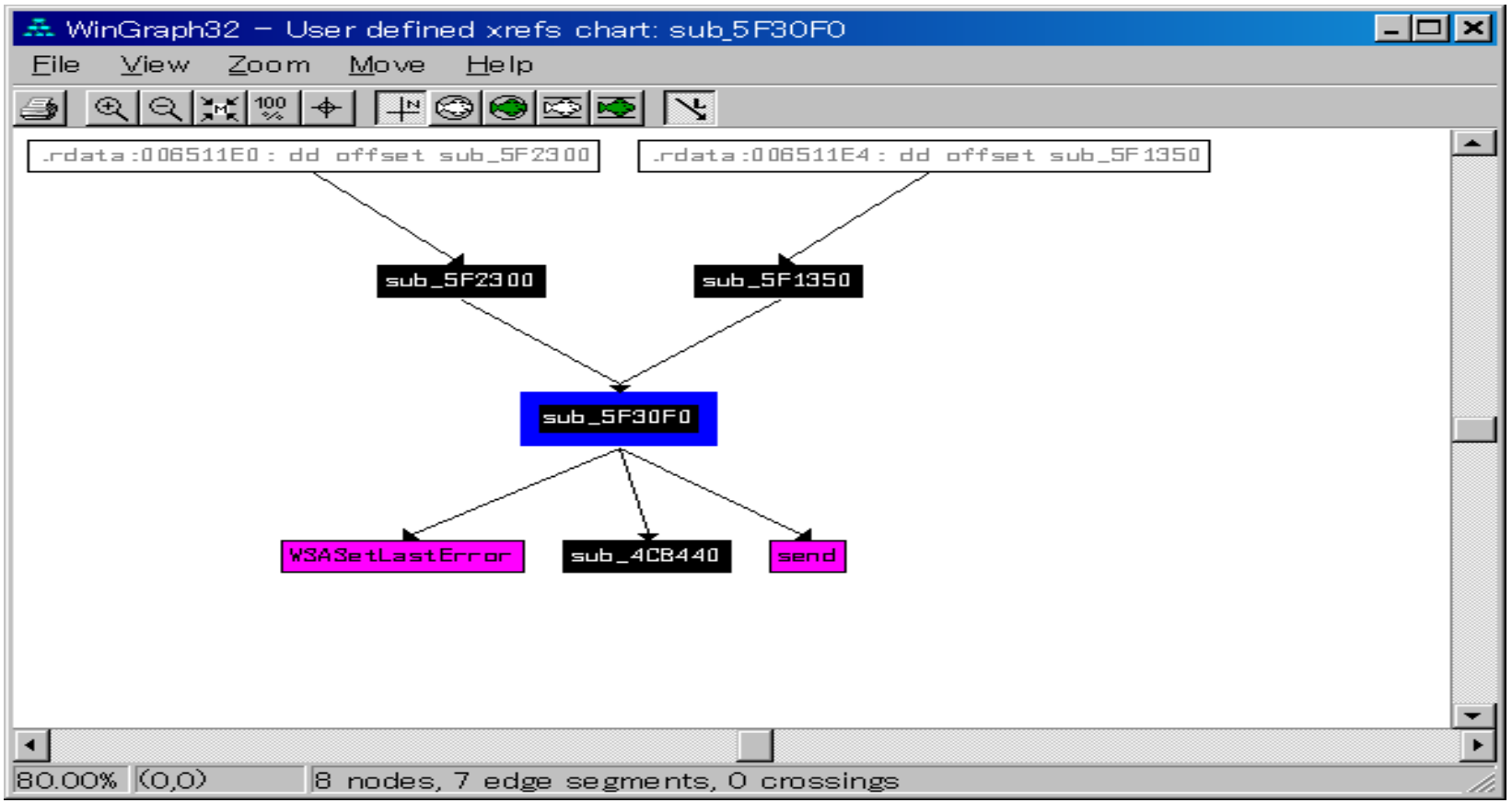
その関数の参照元

ネットエージェント株式会社



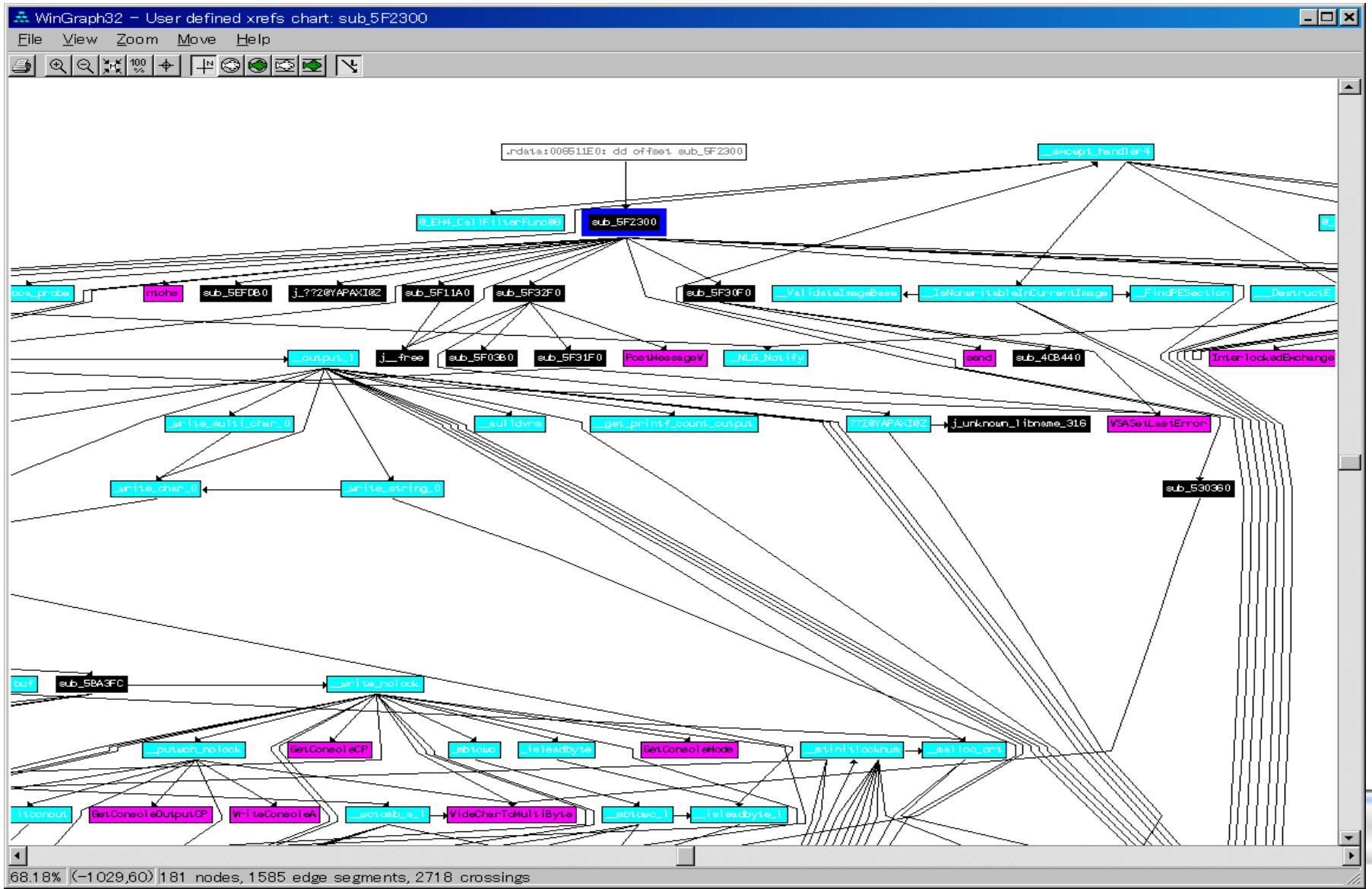
その関数のチャート

ネットエージェント株式会社



1つまえの関数のチャート

ネットエージェント株式会社



動的解析(ollydbg)

NetAgent
ネットエージェント株式会社

- ディバック対策がされていると使えないことがある。
  - ディバッグ対策を回避するメモリパッチを作成
  - Olly上で当てて実行
    - プログラムが不安定になることも多い

呼び元がたどれない所は

NetAgent
ネットエージェント株式会社

- 動的解析をしてブレイクポイントをセットして待つ。
- 呼び元もしくは、サブルーチンの最後まで動かして戻るポイントが呼び元

実際にやってみます。

ネタ探し

NetAgent
ネットエージェント株式会社

- RootkitRevealer
- http://www.microsoft.com/technet/sysinternals/utilities/RootkitRevealer.mspx
  - 自分のPCで発見されても困ります。

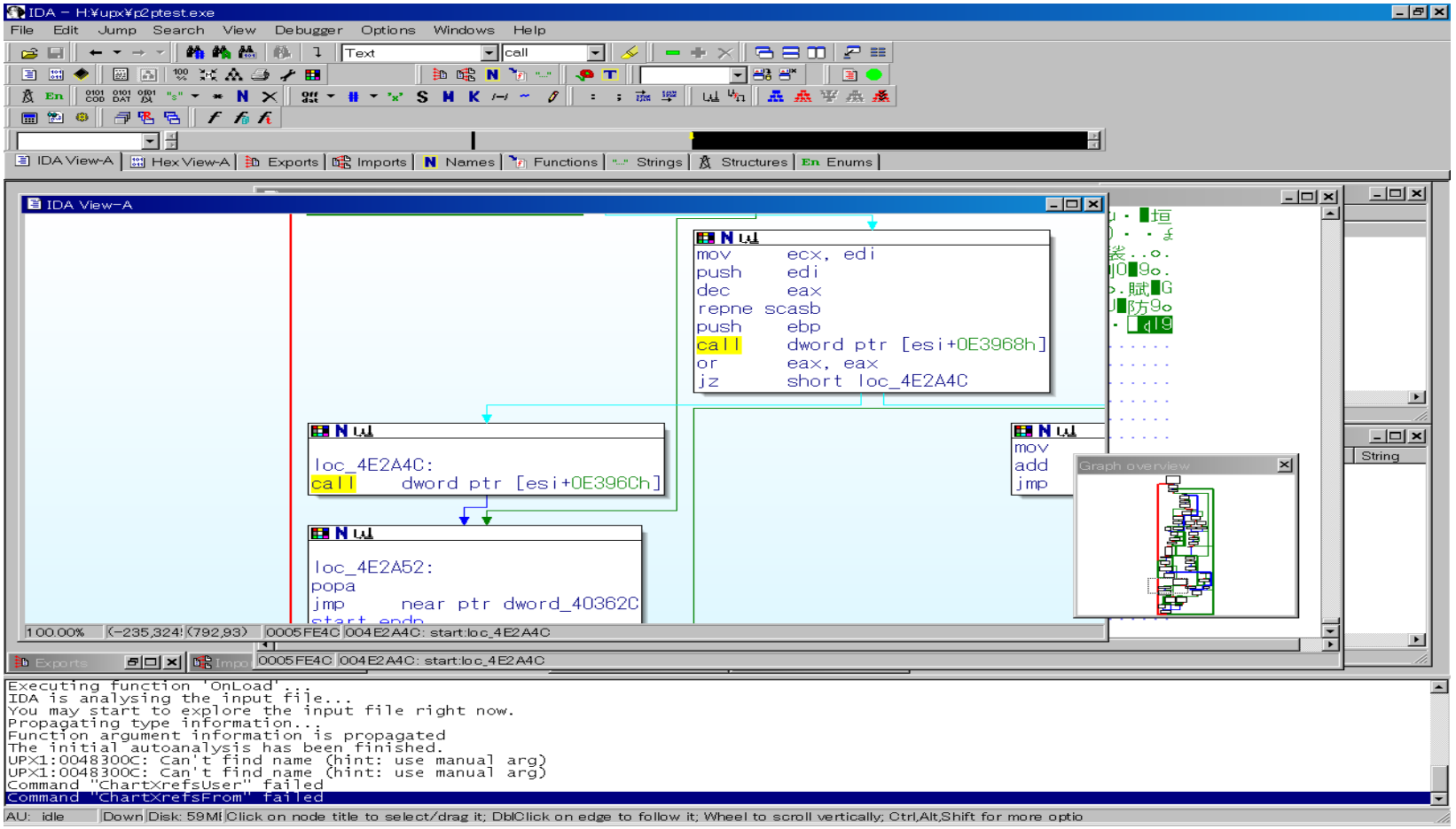
Packer パッカー

NetAgent
ネットエージェント株式会社

- UPX日本語フロントエンド http://www.vector.co.jp/soft/win95/util/se139612.html
- UPX http://upx.sourceforge.net/
- ASPack
- http://www.aspack.com/index.html
- tElock
- http://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/Telock.shtml

UPX

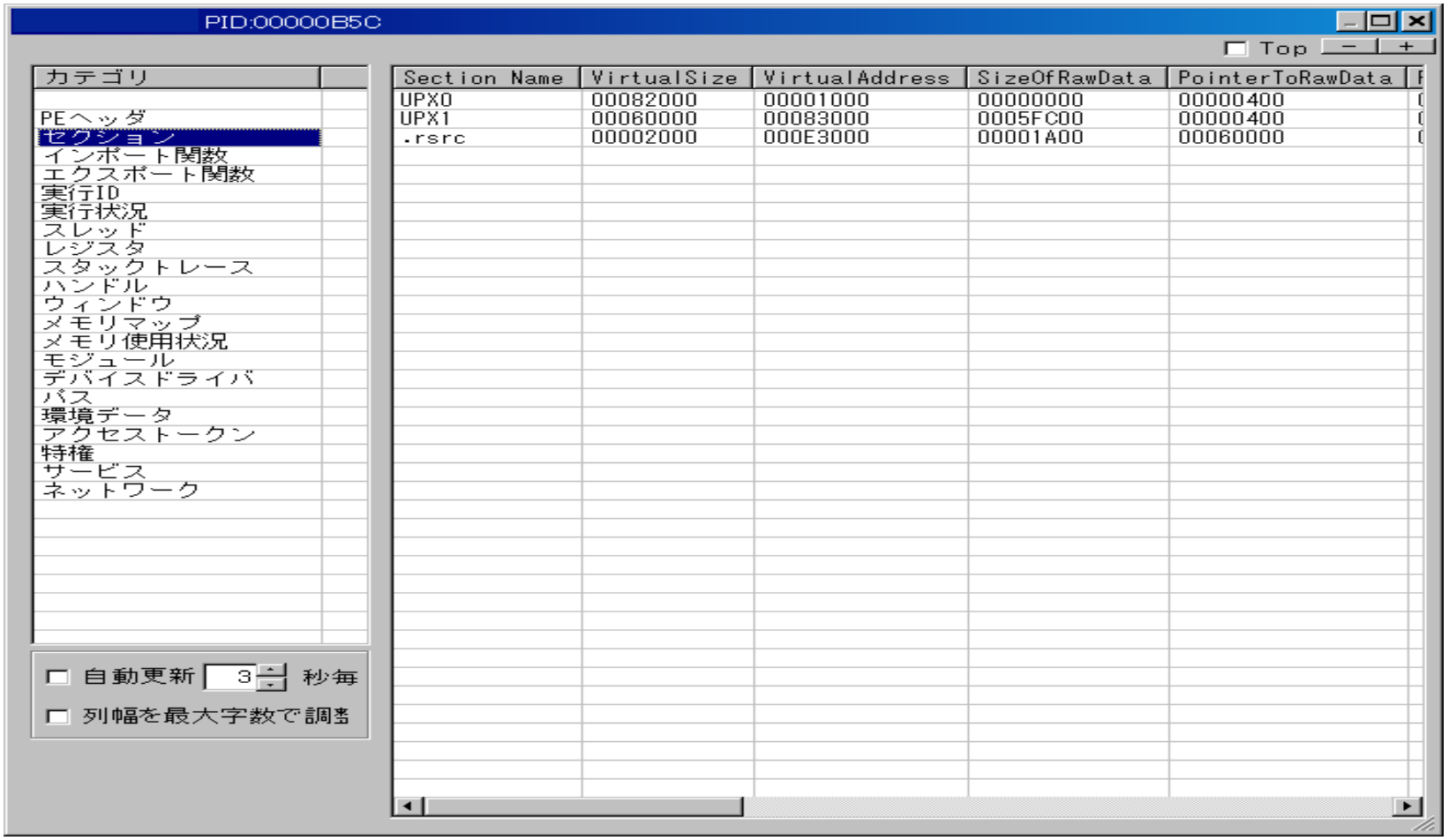
NetAgent
ネットエージェント株式会社



UPXのプログラム構造

UPXうさみみ

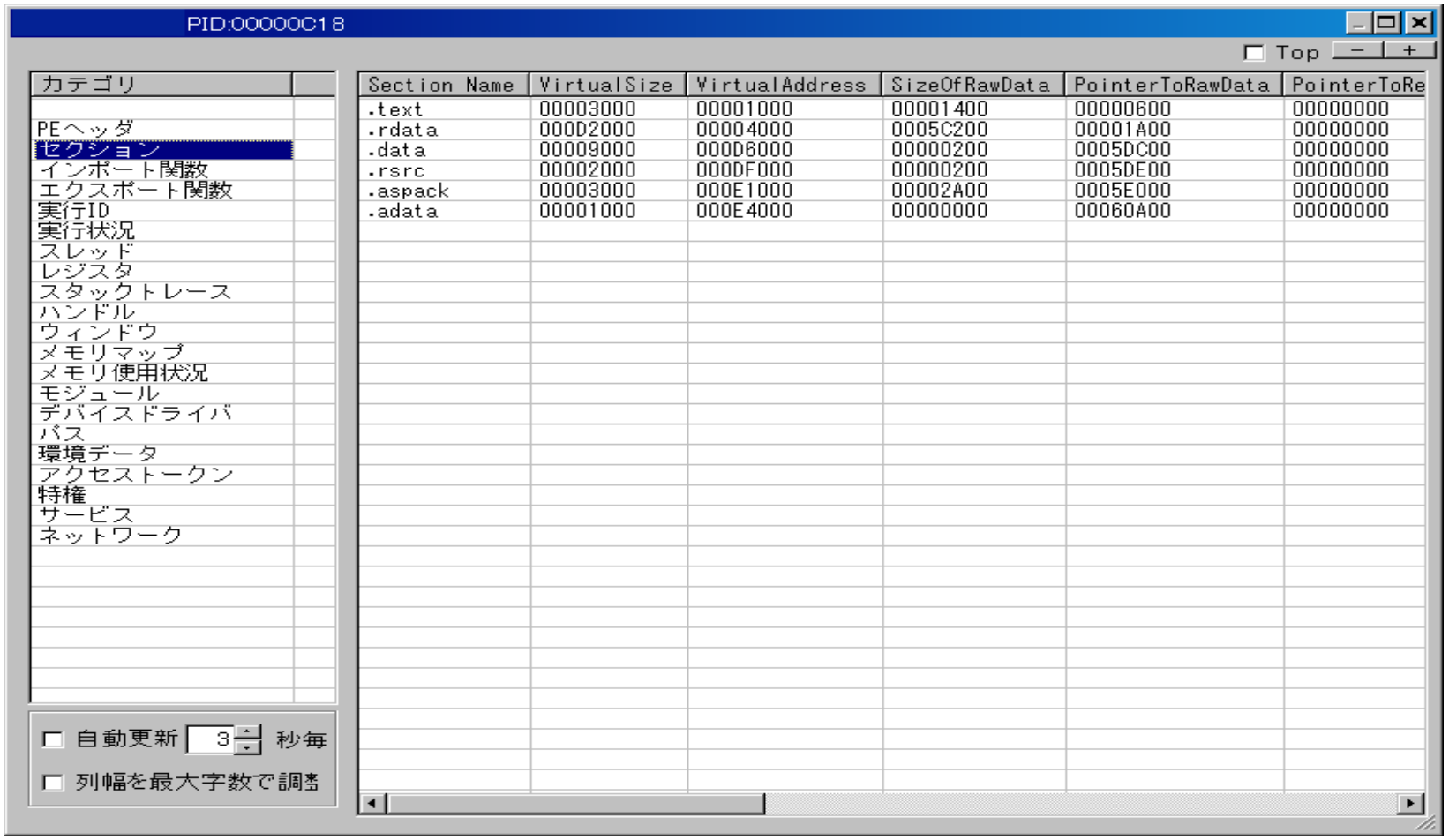
ネットエージェント株式会社



NetAgent **セクション情報で直ぐに分かる**

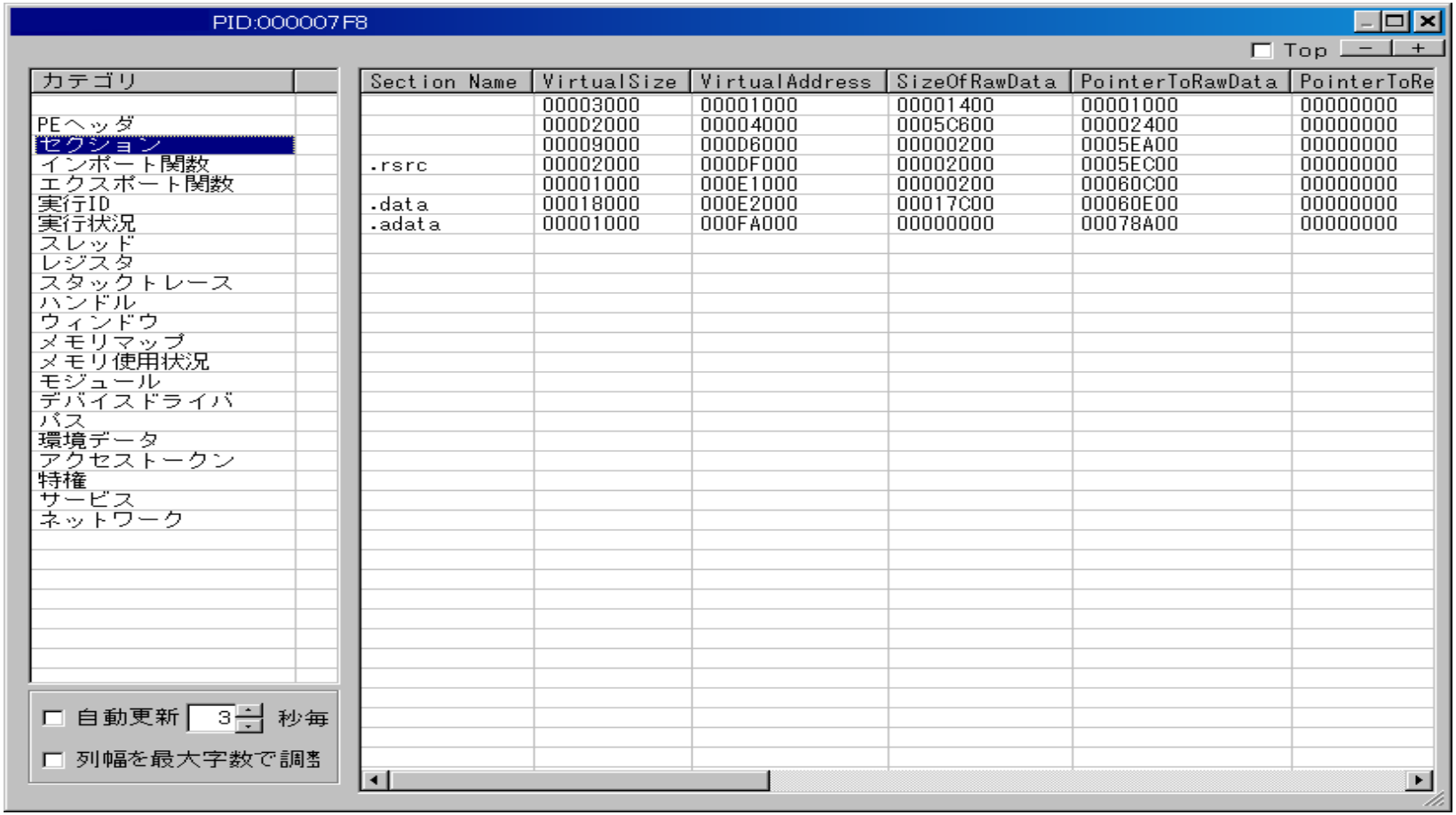
Aspack

ネットエージェント株式会社



ASprotect

NetAgent
ネットエージェント株式会社



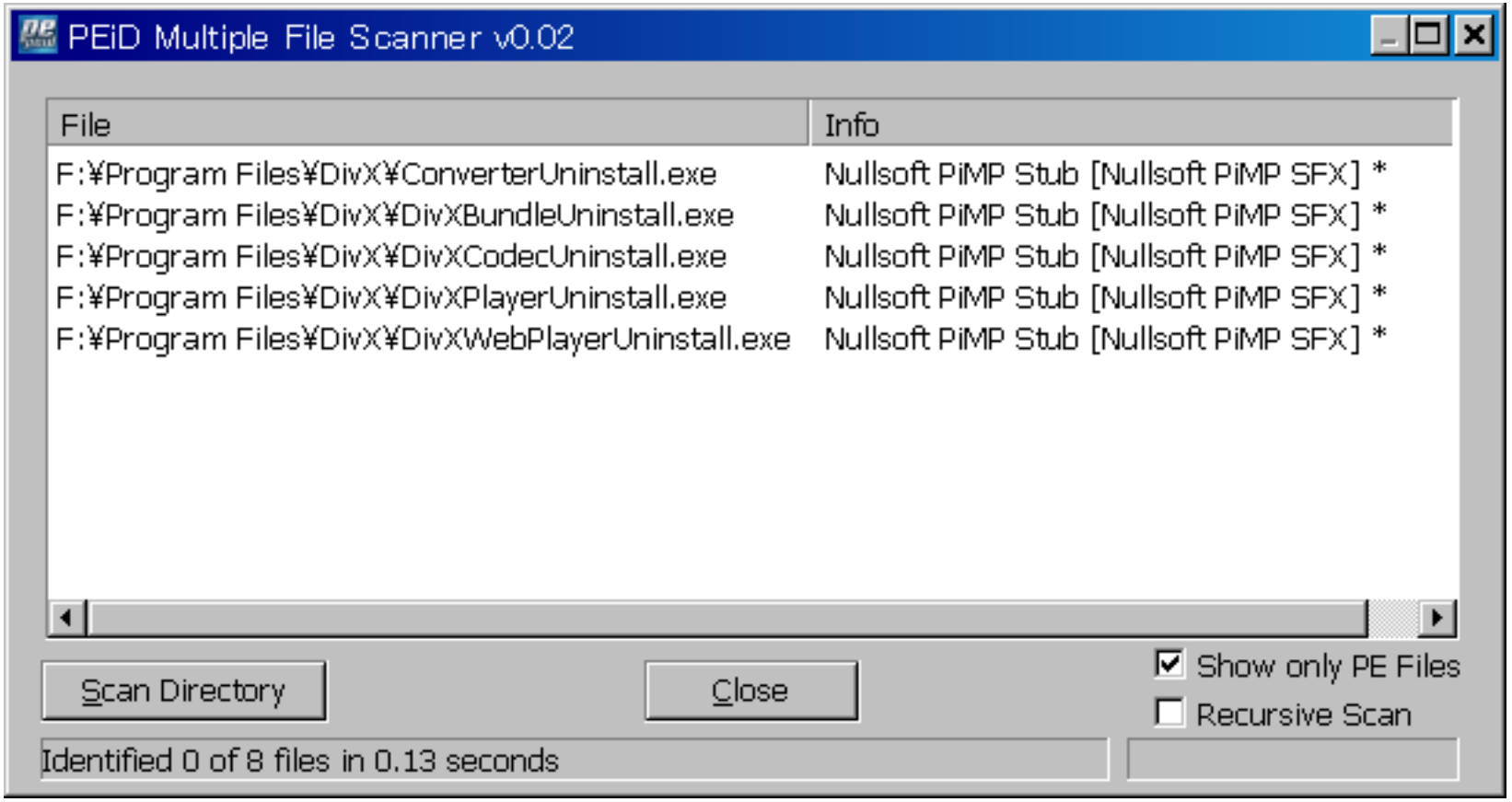
PEiD

NetAgent
ネットエージェント株式会社

- パッカーのチェック
  - http://www.secretashell.com/codomain/peid/
- 結果のサンプル用
  - Lhaplus
  - Winrar
  - DivX
  - Xvid

PEid結果

NetAgent
ネットエージェント株式会社



動的解析とメモリ情報の取得

NetAgent
ネットエージェント株式会社

- Ollyを使ってやってみましょう

暗号サブルーチンの発見(IDA)

NetAgent
ネットエージェント株式会社

- IDAのプラグインであたりをつけましょう。

暗号前のデータを入手

NetAgent
ネットエージェント株式会社

- Ollyでやってみましょう。

まとめ

NetAgent
ネットエージェント株式会社

- バイナリプログラムでもかなり用意に通信内容を解析できます。
- パケットキャプチャでできるならそっちの方が楽にできる。
- 暗号化されていても通信しているプログラムは実態を持っている。


NetAgent